

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of)

(Briefly describe the property to be searched or identify the person by
name and address))

(1) 120 East Road, High Point, New York 12440 and)

(2) The person of Brian Tate, born October 5, 1974)

Case No. 1:25-SW-112 (DJS)

U.S. DISTRICT COURT – N.D. OF N.Y.

FILED

May 16 - 2025

John M. Domurad, Clerk

As further described in Attachments A-1 and A-2

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachments A-1 and A-2

located in the Northern District of New York, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

18 U.S.C. § 875(c)

Offense Description

Interstate Threats

18 U.S.C §§ 922(g)(1)

Possession of Firearm by Prohibited Person

The application is based on these facts:

See accompany affidavit, incorporated herein

☒ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



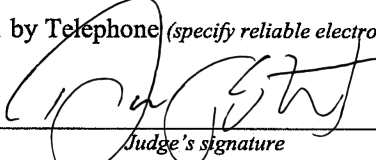
FBI Special Agent Don Zumpano

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone (specify reliable electronic means).

Date: May 16, 2025

City and state: Albany, New York



Hon. Daniel J. Stewart, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCHES OF:

- (1) **120 East Road, High Point, New York 12440 and**
- (2) **The person of Brian Tate, born October 5, 1974**

Case No. 1:25-SW-112(DJS)

As further described in Attachments A-1 and A-2

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Don Zumpano, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search (1) the premises located at **120 East Road, High Point, New York 12440** including any outbuildings, and any closed or locked containers and safes therein, as further described in Attachments A-1 (the “**PREMISES**”), as well as (2) the person of **Brian Tate**, born October 5, 1974, as further described in Attachment A-2, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, currently assigned to the Albany, New York Office. I have been employed as a Special Agent with the FBI since 2009. Since that time, I have been assigned to the FBI New York Division, FBI Headquarters in Washington, DC, and the FBI Albany Division. My assignments have primarily included investigating violations of federal law, including violent criminal offenders, transnational organized crime, narcotics trafficking, crimes against children, and human trafficking. I have also held leadership positions within the FBI, including as a Supervisory Special Agent and Assistant

Special Agent in Charge at the FBI Albany Division. I have participated in the execution of numerous warrants involving the search and seizure of firearms, ammunition, and various other prohibited items.

3. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to execute search warrants for, offenses enumerated in Title 18 of United States Code. I am also a “federal law enforcement officer” within the meaning of Fed. R. Crim. P. 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that **Brian Tate** has made threats in interstate commerce, in violation of 18 U.S.C. § 875(c), and that he illegally possesses firearms in violation of 18 U.S.C. § 922(g)(1). There is also probable cause to search **Tate** and the **PREMISES** for evidence, fruits, and instrumentalities of these crimes as further described in Attachment B.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, investigators, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

The Premises and Person to Be Searched

6. **120 East Road, High Point, New York 12440**, is a one level home with yellow siding, red shutters, a red roof, and a white front door. It is the current residence of **Brian Tate**. A photograph of the exterior of the building is below:



7. **Brian Tate**, born October 5, 1974, is a white male who is approximately 5’8”, weighs approximately 265 pounds, and has brown eyes and is bald.

PROBABLE CAUSE

8. The FBI and the United States Secret Service (USSS) recently became aware of an individual using the social media platform X, formerly known as Twitter, who had posted disturbing statements online via the X user account “@JamesTate121” with the display name “James Tate” (hereafter “the Account”). The statements posted by the Account include statements related to the use of firearms, derogatory statements regarding the President of the United States, and what appear to be threats.

9. Law enforcement investigators reviewed the Account’s online activity on X and observed a publicly-posted statement from April 28, 2025, at approximately 6:44 PM, in which a post from the Account “replied” to another user’s post. The other users post contained a “GIF”

image of President Donald J. Trump's head exploding. The Account's responded "I can do that with a .270 at 300 yards," as seen below:



10. Based on my training and experience, I know that a “.270” is a common type of bolt-action rifle. A review of other posts from the account confirms my understanding, as the Account explicitly refers to a “270 rifle”:



11. Posts from the Account contain numerous references to a .270 owned by the account user. Posts such as “My .270 is ready,” and “My favorite rifle is my 270 MAGA, stop asking.” In one post from December 5, 2024, referring to an article saying “Elon Musk has ‘declared war on Social Security’” the Account user said “Millions of us declare war back.” Then, in response to another user who posted “Fucker has no idea what will hit him,” referring to Mr. Musk, the Account user posted “270 in the back of ear from 300 yards.”



12. Public posts from the Account also contain identifying information, such as that the user is 50 years old, is located in the Hudson Valley region of New York state, and that he is the primary caretaker for three children, two of whom have special needs.

13. Based on the nature of these statements, investigators obtained subscriber information from X Corporation, which indicated that the email associated with the Account was brianate329@yahoo.com. The subscriber information also included an IP address, which law enforcement have not yet traced.

14. Based on the email associated with the Account and the publicly available identifying information, law enforcement identified a **Brian Tate** who resides at 120 East Road in High Falls, New York (the **PREMISES**). Based on my training, experience, and knowledge of the investigation, it appears James Tate is Brian Tate's son with down syndrome. For example, publicly available information, including a public fundraiser on the website "GoFundMe," indicates that Tate's son is named James.

15. Brian Tate is a convicted felon who, on April 30, 1998, pled guilty in Clinton County Court to criminal sale of a controlled substance in the fifth degree, in violation of New York State Penal Law Section 220.31, and was sentenced to a 16 month-to-4-year term of imprisonment.

16. On May 13, 2025, I traveled to the PREMISES with a special agent from the USSS and a New York State Police Investigator to interview Tate about his social media posts. Tate admitted that he made the posts from the Account. Tate further told us that he sometimes vents on social media due to the stress from his children, particularly when he is drinking alcohol, and claimed he didn't mean anything from his posts. He also told us that he does not possess a firearm.

Tate admitted that he had been previously arrested for distribution of marijuana. Law enforcement did not search the home on May 13, 2025.

* * *

17. In my training and experience, individuals that threaten others on the internet, particularly when the circumstances involve politics, often maintain anti-President propaganda or other evidence of their personal biases in their residences. For instance, as to President Biden, many of those that have previously threatened the President maintain memorabilia or clothing labeled with “Let’s Go Brandon” as a stand-in phrase for “Fuck Joe Biden.” Furthermore, individuals who make their threats online often do so via electronic means on computers, phones, or tablets which are found within their residences. Likewise, records and evidence indicating who lives at or has maintained control of the residence, including during the time frame during which the threats were made, are likely to be found within the residence. Here, given **Tate** admitted to making the posts, information on the computer equipment within **PREMISES** could verify the location where the threat was placed from. I accordingly seek authorization to search all structures, residences, rooms, garages, storage areas, sheds, and vehicles under the control of the owners, occupants, and/or possessors of the **PREMISES** at the time of the execution of the search warrant.

18. Given the prevalence of references to a “.270” on Tate’s social media, I submit there is probable cause to believe that firearms are being stored at **the PREMISES**. Possession of firearms by a prohibited person, particular one who is actively making threats on the internet, presents an obvious risk to the safety of the would-be-targets and others around Tate.

19. In my training and experience, those that threaten others online frequently use cellphone-based methods of communications, including text messages, to effectuate their threats and to share their personal biases with similarly minded individuals. As set forth above, the posts

in this case where made on a social media platform, X, which is a commonly used application found on cell phones. Those that use social media regularly keep their cellphones on their person, in their vehicles, in their residences and at locations under their control.

20. In my training and experience, individuals involved who illegally possess firearms or will often conceal, store, and transport those firearms in vehicles under their control. Often, therefore, such individuals will have several vehicles located on or near their properties. When checking with the Department of Motor Vehicles, agents and law enforcement officers will often find that such vehicles are registered in the names of other individuals. This is often the result of criminals' attempts to insulate themselves should the vehicles be found containing drugs or other contraband. Likewise, documents such as ownership information, orders of protection, invoices, receipts, cancelled checks, bank records, and other evidence may be found in the vehicles. Based on my training, experience, and knowledge of the investigation, I believe that searching vehicles present at the **PREMISES** and found to be under the control of **Tate** during the service of the search warrants may produce relevant evidence, including but not limited to controlled substances, currency, and records relevant to the threats and firearms violations under investigation.

TECHNICAL TERMS

21. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be

directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

22. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **PREMISES** or **Tate**, in whatever form they are found. One form in which the records might be found is data stored on a cell phone, tablet, computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

23. *Probable cause.* I submit that if a computer, cell phone, table, or storage medium is found on the **PREMISES** or **Tate**, there is probable cause to believe those records will be stored on that computer, cell phone, tablet, or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
- e. Based on actual inspection of other evidence related to this investigation, including social media records, I am aware that computer equipment was used to generate the

posts at issue. There is reason to believe that there are computer systems currently located on the **PREMISES** or Tate, at least in the form of cellular phones or other small portable electronic devices.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **PREMISES** or on Tate because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where,

and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculping or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically

also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore,

contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to access bank accounts, shipment records, and other financial information, or to access an application over which a threat was made, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

25. *Necessity of seizing or copying entire computers, cell phones, tablets, or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a

complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying computers, cell phones, tablets, and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

27. Because several people share the **PREMISES**, it is possible that the **PREMISES** will contain computers, cell phones, tablets, or storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

28. *Biometric unlocking of devices.* The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

- d. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many

electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

- e. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.
- f. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called “Face ID.” During the Face ID registration process, the user holds the device in front of his or her face. The device’s camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

- g. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- h. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.
- i. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions.

Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- j. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual who is found at the **PREMISES** and reasonably believed by law enforcement to be a user of the device, as well as **Tate**, to unlock the device using biometric features in the same manner as discussed above.
- k. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual who is found at the **PREMISES** and reasonably believed by law enforcement to be a user of the device, as well as **Tate**, to the fingerprint


scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

CONCLUSION

29. Based on the forgoing, there is probable cause to believe that the **PREMISES** described in Attachment A-1, and **Tate**, further described in Attachment A-2, and respectively incorporated herein by reference, will contain items set forth in Attachment B. These items constitute evidence of the commission of criminal offenses and contraband, fruits of the crime, things otherwise criminally possessed, and property designed or intended for use or that is or has been used as the means of committing the criminal offenses of 18 U.S.C. § 875(c) (interstate threats); and 18 U.S.C. § 922(g)(1) (illegal possession of a firearm by prohibited persons) by Brian Tate. I therefore respectfully request that the Court issue the proposed search warrants.

Attested to by the affiant.

Respectfully submitted,


Don Zumpano
Special Agent
Federal Bureau of Investigation

I, the Honorable Daniel J. Stewart, United States Magistrate Judge, hereby acknowledge that this affidavit was attested to by the affiant by telephone on May 16, 2025, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.



Hon. Daniel J. Stewart
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to be searched

The property to be searched is **120 East Road, High Point, New York 12440**, and any locked or closed containers and safes therein, any outbuildings or sheds (referred to as the “PREMISES”), and any and all vehicles owned, leased, rented, or operated by residents of the PREMISES parked on or near the PREMISES at the time of the service of the search warrant.

The PREMISES is more fully described as a one level home with yellow siding, red shutters, a red roof, and a white front door. It is the current residence of **Brian Tate**. A photo of the exterior of the building and the attached garage are below:



ATTACHMENT A-2

Person to be searched

The person to be searched is **Brian Tate**, born October 5, 1974, and any and all vehicles owned, leased, rented, or operated by Tate at the time and place of the search. **Tate** is a white male who is approximately 5'8", weighs approximately 265 pounds, and has brown eyes and is bald.

ATTACHMENT B

Items to be seized

1. All evidence, fruits, and instrumentalities of violations 18 U.S.C. § 875(c) (interstate threats); and 18 U.S.C. §§ 922(g)(1) (illegal possession of a firearm by prohibited persons), by **Brian Tate**, and occurring on and after January 1, 2024:
 - a. Evidence concerning ownership or occupancy of **120 East Road, High Falls, New York 12440**, including utility and telephone bills, mail envelopes, addressed correspondence, diaries, statements, identification documents, address books, and telephone directories.
 - b. Evidence involving any personal animus towards Elon Musk, including clothing, memorabilia, pictures, personal journals, notebooks, or other writings.
 - c. Records related to the use of firearms, such as communications, ledgers, records relating to the purchase of firearms, paraphernalia and other instrumentalities of the offense, and contact information for firearms sellers.
 - d. Firearms, ammunition, containers for firearms or ammunition, and other firearms paraphernalia, including targets, cleaning supplies, and documents and communications relating to firearms or ammunition.
 - e. Surveillance items, such as cameras, closed circuit televisions, scanners, radios, and other recording devices.
2. Cell phones, tablets, or storage media that may contain any electronically stored information falling within the categories set forth in Sections (1)(a)-(i), above. In lieu of seizing any such devices this warrant also authorizes the copying of such devices or media for later review.

In searching the electronic devices seized pursuant to this warrant, law enforcement personnel are further authorized to seize:

- i. Information and records establishing the identity of the person who used the electronic device;
- ii. Information related to the location of the electronic device and/or its user at the times of the crimes under investigation; and
- iii. Information evidencing the user of the device's state of mind as it relates to the crimes under investigation.

Use of Fingerprints and Face

During the execution of this search warrant, law enforcement personnel are authorized to press the fingers (including thumbs) of Brian Tate to the fingerprint sensor of any smartphones or electronic devices seized in connection with this warrant for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. During the execution of this search warrant, law enforcement personnel are authorized to have Tate remain still and look, with eyes open, at the camera of any smartphones or electronic devices seized in connection with this warrant for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

Review of Electronically Stored Information ("ESI")

Following seizure of any electronic device and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example: surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the cellphone was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Sections (1) and (2) of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted

by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the Federal Bureau of Investigation may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.